REMARKS

Claims 1-21 are pending in the application prior to entry of this Amendment.

Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ananian et al (US 2003/0028451) in view of Boyce et al. (6,934,838).

Claims 18 and 19 are voluntarily amended hereby to delete any extraneous periods (.) within the interior body of the claims. Claim 1 is voluntarily amended hereby to correctly reference an antecedent basis in the "resident application" element. Claim 7 is voluntarily amended hereby to correctly reference the intervening claim 2's "system" instead of its "database operation". Claims 15-21 are voluntarily amended hereby at the Examiner's suggestion to properly reference in their preambles "a machine-executable medium comprising instructions that, when executed by a machine, cause the machine to" perform the recited steps. Finally, claim 21 is voluntarily amended hereby to change its paragraphing format and to omit an unnecessary "and" between the first and second of the four recited elements.

New claims 22 and 23 are added hereby and are directed to further limitations of the system recited in claim 1. No new matter is added, as such features as quarantine memory contents including an unencrypted personal record and an unencrypted personal key are described and illustrated in Figs. 2-4 and at paragraphs **[00028]** and **[00033]** of the specification as originally filed.

Applicant thanks the Examiner for pointing out the objectionable claims and submits that all pending claims, as amended hereby, are now definite and unobjectionable. No new matter is added, and the amendments should be entered.

Claims 1-23 after entry of this Amendment are presented for consideration and allowance.

Claim Rejections – 35 U.S.C. § 103

Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ananian et al in view of Boyce et al.

First, applicant deems Boyce et al. to be only 35 USC 102(e) prior art against applicant's present application. Applicant does not concede priority of the Boyce et al. disclosure patented after applicant's filing date, and applicant reserves the right to swear behind Boyce et al.

GENERAL DISCUSSION

Applicant disputes the Detailed Action's characterization of the present invention (hereinafter "Thorson") as "obvious" under 35 U.S.C. 103(a), given the teachings of Ananian in view of Boyce. This characterization (Detailed Action paragraphs #4 and 5) is the foundation for all of the specific assertions of obviousness (paragraphs 6-19) on which the rejection is based.

As the Detailed Action points out, the three systems in question share certain vaguely common elements. All involve a plurality of individual users, a plurality of entities with whom they communicate, and an intermediary which arranges and secures such communication. All three provide some degree of protection of the user's privacy against unauthorized access by outside parties, and some form of anonymization of the user's identity. Each maintains a user database containing information that users might wish kept private.

Beyond that, however, similarities between the prior art and the present invention break down. In comparing the present invention with Boyce and Ananian, the Detailed Action appropriates the present invention's terminology, in some cases mapping it vaguely onto the two prior art inventions, thereby overstating similarities, downplaying differences, and conflating elements which, though superficially similar, are used in divergent ways as required by the disparate purposes of the three respective systems.

The critical characteristic that distinguishes the present invention from Boyce and Ananian is the extra degree of privacy the present invention affords users by treating the server-side intermediary ("Anonymity Service") as an *untrustworthy outsider* ("a central characteristic of all embodiments... is the inability of Anonymity Service 130 to access Subject's 120 unencrypted personal data" [0034]).

This design premise is paradoxical within a customary network-design context, in which "trustworthiness" is commonly imputed to server-side components (by virtue of closer supervisory control and concentrated security arrangements), while client-side components are more typically regarded as suspect. Inverting this paradigm induces architectural and procedural contortions of a highly counterintuitive nature, yielding an architecture which "a person having ordinary skill in the art" would more likely regard as obtuse, complex, contrary, perplexing, unwieldy, burdensome and inefficient than "obvious."

Of course, as the present application illustrates, such a counter-intuitive approach that turns the prior art paradigm on its head also yields increased subject data security and subject anonymity.

Assume it would be possible to implement a system based on the teachings of Ananian, extended with the security enhancements taught by Boyce, without encountering insurmountable difficulties. Assume further that it does not matter whether we imagine the resulting hybrid system (hereinafter referred to as "the hybrid system") as the result of incorporating

- Ananian into Boyce such that CSS 200 (Ananian Fig. 2) becomes Service Provider 20 (Boyce Fig. 1), and ICG 221 and ICA 222 (Ananian Fig. 2) become Service Applications 40 (Boyce Fig. 1);
- Ananian into Boyce such that Ananian's CSS 200 becomes one of Boyce's Service Applications 40, of which Ananian's ICG 222 and ICA 222 are internal components; or
- Boyce into Ananian, perhaps becoming a new entity within the Presentation layer (Ananian Fig. 2), intercepting the two arrows connecting User 111 with ICG 221 and ICA 222.

The inverted nature of the Thorson invention creates fundamental incompatibilities with the resulting hybrid system because, like both its prior art antecedents, the Examiner's hybrid system produced by combining the Boyce and Ananian references embodies the server-centric trust model from which Thorson is a drastic departure. Applicant asserts that overcoming these incompatibilities to create the message targeting and database system described in Thorson (MTDBMS) would require changes so structurally deep-rooted as to nullify either (a) the defining premises of the hybrid system (including key features foundational to both Boyce and Ananian), or (b) the "untrustworthy intermediary" premise underlying Thorson.

The inverted client-centric privacy model underlying Thorson teaches explicitly and in detail how its "untrustworthy intermediary" premise is to be implemented by strict client-side sequestration of two critical elements of user privacy:

- the user's self-descriptive profile and message filtering policy (Personal Record 110, which is Encrypted PR 109 in its unencrypted form), and
- the private half of the dual key (Private Key 211, which is Encrypted Private Key 213 in its unencrypted form) required for decrypting Encrypted PR 109.

Neither of these elements is sequestered in the client in either Boyce or Ananian. Applicant further asserts that no such client-side sequestration can be inferred from either prior art antecedent, and consequently no such sequestration can be fairly inferred from a "hybrid" system based on their teachings.

Each of independent claims 1, 8, and 15 recites these important sequestration features in slightly different ways. Claim 1 recites "a resident application residing on a client device under control of the subject, the resident application *managing access to the personal record* in an unencrypted state; a quarantine memory, the quarantine memory *being a secure area of system memory on the client device*; and a session agent to perform a database operation on the personal record in the unencrypted state *in the quarantine memory*." Claims 8 and 15 recite "maintain[ing] a personal record belonging to a subject in a centralized database *in an encrypted form* ... ; and distribute[ing] a database operation from the centralized database to a client device when the database operation is performed on the personal record *in an unencrypted form*." Thus, all pending claims are submitted already as being patentably distinctive over the prior art.

User profile: In a hybrid system, user information (apart from security credentials) would be the province of Ananian. Applicant observes that, contrary to the sequestration approach taken by Thorson,

a. User profile data is managed entirely on the server side. Ananian relies entirely on *anonymization* to preserve user privacy, and nowhere envisions, suggests, anticipates or implies any form of client-side sequestration of user identity, profile, or other data. All of Ananian's marketing functions, such as aggregation of response data, behavior tracking, demographic data mining, and peer sharing occur inside the server perimeter, where they enjoy the concentrated security and efficiency afforded by customary server-side database deployment.

Nothing in Ananian suggests or anticipates anything resembling Thorson's distributed *permission query*, in which a message broadcast instigates a piecewise query of the entire user database, seeking prior delivery permission from *all* users, one client device at a time. See claims 2, 3, 12, 13, 19, and 20. Nor would there be any reason for inventing such an unorthodox operation in a system which relies entirely on anonymity for its privacy assurance. "Targeting and filtering," to the extent that they have analogs in Ananian, have very different purposes. "Filtering" is actively instigated by a user's request for published catalog data, which returns a view customized according to his preferences. "Targeting" applies only to follow-up communications that may result from behavior tracking by a vendor after the primary "message" has been delivered. Both "targeting and filtering" occur in any case entirely on the server side, albeit being performed on anonymized data.

Applicant asserts that these fundamental differences alone render the teachings in Thorson non-obvious to a student of Ananian.

However, assuming the contrary for argument's sake, suppose a "person of ordinary skill in the art" has independently formed the same intent as Thorson without prior exposure to Thorson's teachings, and seeks to achieve the "untrustworthy intermediary" standard by anonymization alone. He must still learn from Ananian, or discover by obvious inference, how to implement it.

b. Ananian, despite total reliance on anonymity for preserving user privacy, is consistently vague about how and where anonymization is initiated and managed. Clearly anonymization requires knowledge of *both* the user's identities, so this detail is central to any reassurance that user data is being concealed from the "untrustworthy intermediary."

c. Ananian teaches anonymity of user profile data, without teaching any particular apparatus or method for assigning an anonymous identity, binding it uniquely and persistently to a user's real-world identity, and concealing that mapping from the server-side elements of Ananian.

d. Turning to Ananian's drawings and detailed description for guidance, the skilled artisan would have great difficulty seeing how to implement such anonymity.

Note that Boyce, while claiming the ability to "anonymize" a user's identity (by which is meant concealment from outside parties), makes no attempt to conceal it from the service application with which he is conducting secure communications. In fact, Boyce *requires* the user to have established a prior independent relationship with the service application, details of which relationship are the basis for creating authentication credentials. Hence Boyce provides no help in achieving the kind of anonymity required by Ananian.

Ananian Fig. 2 offers no guidance in understanding where the anonymity function resides, let alone how to build it. Clearly it would have to be interposed somewhere between Actors 110 and the ICA 222 which are components of the Presentation layer 220 and embody the Actors' user interface to the Catalog Server System (CSS 200). In other references, Ananian refers to an "IDCP account" and PIN, and declares [0512] that "the CSS 200 keeps the User's identity anonymous by not merging the IDCP account number with any PII" (personally identifying information), suggesting that anonymity is conferred by the IDCP. This entity (the "Interactive Digital Catalog